#3 Priority 3/6/01

Docket No. 826.1657 (JDH)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

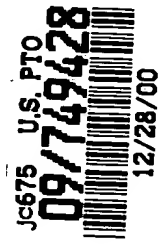
Isao YAGASAKI, et al.

Serial No.: To be assigned

Filed: December 28, 2000

Group Art Unit: Unassigned

Examiner: Unassigned



For: **CERTIFICATING SYSTEM FOR PLURALITY OF SERVICES AND METHOD THEREOF**

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. §1.55

Assistant Commissioner for Patents
Washington, D.C. 2023l

Sir:

In accordance with the provisions of 37 C.F.R. §1.55, the applicants submit herewith a certified copy of the following foreign application:

Japanese Patent Application No. 2000-121581
Filed: April 21, 2000.

It is respectfully requested that the applicants be given the benefit of the foreign filing date as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. §119.

Respectfully submitted,

STAAS & HALSEY LLP

By: _____
James D. Halsey, Jr.
Registration No. 22,729

Date: December 28, 2000
700 11th Street, N.W., Ste. 500
Washington, D.C. 20001
(202) 434-1500

PATANT OFFICE
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: April 21, 2000

Application Number: Patent Application
No. 2000-121581

Applicant(s): FUJITSU LIMITED

September 29, 2000

Commissioner,
Patent Office Kozo OIKAWA

Certificate No. 2000-3079682

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年 ４月２１日

出 願 番 号
Application Number: 特願２０００－１２１５８１

出 願 人
Applicant (s): 富士通株式会社

２０００年 ９月２９日

特 許 庁 長 官
Commissioner,
Patent Office 及 川 耕 造

出証番号 出証特２０００－３０７９６８２

【書類名】　特許願

【整理番号】　0050269

【提出日】　平成12年 4月21日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 15/00

H04L 9/32

【発明の名称】　複数のサービスのための認証システムおよび方法

【請求項の数】　7

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　矢ケ崎　功

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　黒田　俊光

【特許出願人】

【識別番号】　000005223

【氏名又は名称】　富士通株式会社

【代理人】

【識別番号】　100074099

【住所又は居所】　東京都千代田区二番町８番地２０　二番町ビル３Ｆ

【弁理士】

【氏名又は名称】　大菅　義之

【電話番号】　03-3238-0031

【選任した代理人】

【識別番号】　100067987

【住所又は居所】　神奈川県横浜市鶴見区北寺尾７－２５－２８－５０３

【弁理士】

【氏名又は名称】　久木元　彰

【電話番号】　045-573-3683

【手数料の表示】

【予納台帳番号】　012542

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9705047

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　複数のサービスのための認証システムおよび方法

【特許請求の範囲】

【請求項１】　複数のサービスに共通の証明書情報を登録する登録手段と、

ユーザが前記複数のサービスのうちの１つのサービスにアクセスするとき、該ユーザの証明書情報を受け取る受信手段と、

前記ユーザの証明書情報が前記共通の証明書情報に対応するか否かを判定する判定手段と、

前記ユーザの証明書情報が前記共通の証明書情報に対応するとき、前記１つのサービスの利用を許可する許可手段と

を備えることを特徴とする認証システム。

【請求項２】　前記１つのサービスのための識別情報とパスワード情報を格納する格納手段と、該識別情報とパスワード情報に基づいて前記ユーザを認証する認証手段と、該ユーザが認証されたとき、前記共通の証明書情報を該ユーザに発行する発行手段とをさらに備えることを特徴とする請求項１記載の認証システム。

【請求項３】　前記１つのサービスのための識別情報とパスワード情報を格納する格納手段と、該識別情報とパスワード情報に基づいて前記ユーザを認証する認証手段と、該ユーザが認証されたとき、前記共通の証明書情報を失効させる失効手段とをさらに備えることを特徴とする請求項１記載の認証システム。

【請求項４】　前記複数のサービスを、前記共通の証明書情報により利用可能なサービスとして登録する利用サービス管理手段をさらに備えることを特徴とする請求項１記載の認証システム。

【請求項５】　ユーザが１つのサービスにアクセスするとき、該１つのサービスを含む複数のサービスに共通の証明書情報を送出する送信手段と、

前記共通の証明書情報に基づいて前記ユーザが認証されたとき、前記１つのサービスの提供を受けるサービス利用手段と

を備えることを特徴とする端末装置。

【請求項６】　コンピュータのためのプログラムを記録した記録媒体であっ

て、

前記プログラムは、

ユーザが１つのサービスにアクセスするとき、該ユーザの証明書情報を受け取り、

前記ユーザの証明書情報が、あらかじめ登録された、前記１つのサービスを含む複数のサービスに共通の証明書情報に対応するか否かを判定し、

前記ユーザの証明書情報が前記共通の証明書情報に対応するとき、前記１つのサービスの利用を許可する

処理を前記コンピュータに実行させることを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項７】　複数のサービスに共通の証明書情報をあらかじめ登録し、

ユーザが前記複数のサービスのうちの１つのサービスにアクセスするとき、該ユーザの証明書情報が前記共通の証明書情報に対応するか否かを判定し、

前記ユーザの証明書情報が前記共通の証明書情報に対応するとき、該ユーザに対して前記１つのサービスの利用を許可する

ことを特徴とする認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、インターネット等のネットワークを介したサービスに係り、ユーザが複数のサービスを利用する際に、ユーザ認証を行う認証システムおよびその方法に関する。

【０００２】

【従来の技術】

ネットワーク上のサービスを提供する提供者は、サービス料金の課金等のために、アクセスしてきたユーザの認証を行う必要がある。従来のサービスシステムでは、１人のユーザが複数のサービスを利用する場合、各サービスが指定する認証方法をユーザ自らが使い分けていた。

【０００３】

図１４は、このような従来のサービスシステムを示している。２つのサービスＡ、Ｂを利用するとき、ユーザ１１は、まず、サービスＡ用の識別情報（ＩＤ）とパスワード（ＰＷＤ）をサービスＡのサーバ１２に送る。サーバ１２は、ユーザ管理データベース（ユーザ管理ＤＢ）１３を参照してユーザ認証を行った後、ユーザ１１にサービスＡを提供する。

【０００４】

次に、ユーザ１１は、サービスＢ用のＩＤおよびパスワードをサービスＢのサーバ１４に送る。サーバ１４は、ユーザ管理ＤＢ１５を参照してユーザ認証を行った後、ユーザ１１にサービスＢを提供する。こうして、ユーザ１１は、ネットワークサービスＡ、Ｂを利用することができる。

【０００５】

【発明が解決しようとする課題】

しかしながら、上述した従来のサービスシステムには、次のような問題がある。

【０００６】

１人のユーザが複数のネットワークサービスを利用する場合、各サービスが発行するＩＤおよびパスワードを使い分ける必要があり、非常に不便である。特に、サービス毎に異なるＩＤおよびパスワードを用いる場合、ユーザは複数のＩＤおよびパスワードを記憶しておき、サービス利用時に端末から入力しなければならない。したがって、利用サービスの数が多くなると、ユーザの負担が増大する。

【０００７】

また、従来のＩＤおよびパスワードによる認証方法に基づいて、１つのサービスがユーザのＩＤおよびパスワードを登録し、ユーザがそれらを用いて他のサービスを利用することも考えられる。しかし、各サービスの事業体が異なれば、異なる事業体間で互いにパスワードを教え合うことになり、このような認証方法は、セキュリティの観点から、事実上、実現が困難である。

【０００８】

本発明の課題は、複数のサービスのための認証処理において、各サービスが発

行しているパスワード等を互いに知らせることなく、ユーザの負担を軽減する認証システムおよびその方法を提供することである。

【０００９】

【課題を解決するための手段】

図１は、本発明の認証システムの原理図である。図１の認証システムは、登録手段２１、受信手段２２、判定手段２３、および許可手段２４を備える。

【００１０】

登録手段２１は、複数のサービスに共通の証明書情報を登録する。受信手段２２は、ユーザがそれらの複数のサービスのうちの１つのサービスにアクセスするとき、そのユーザの証明書情報を受け取る。判定手段２３は、受け取ったユーザの証明書情報が、登録された共通の証明書情報に対応するか否かを判定する。許可手段２４は、ユーザの証明書情報が共通の証明書情報に対応するとき、アクセスされたサービスの利用を許可する。

【００１１】

ユーザは、あらかじめ発行された、複数のサービスに共通の証明書情報を保持しており、それらのサービスのうちの１つを利用するとき、ユーザ端末から証明書情報を送出する。

【００１２】

受信手段２２は、送られた証明書情報を受け取ると、その情報を判定手段２３に渡し、判定手段２３は、受け取った証明書情報を、登録手段２１に登録された証明書情報と比較して、両者が互いに対応するか否かを判定する。判定結果は許可手段２４に渡され、許可手段２４は、判定結果が２つの証明書情報が互いに対応することを示していれば、ユーザに対してサービスの利用を許可する。

【００１３】

このような認証システムによれば、ユーザは、各サービス固有のＩＤおよびパスワードの代わりに、単一の証明書情報を用いて、複数のサービスを利用することができる。したがって、複数のＩＤおよびパスワードを扱う必要がなくなり、ユーザの負担が軽減される。

【００１４】

例えば、図１の登録手段２１は、後述する図２のユーザ情報管理テーブル３６、３７に対応し、図１の受信手段２２、判定手段２３、および許可手段２４は、図２のサーバ３２、３３に対応する。あるいはまた、図１の登録手段２１は、図２の証明書管理ＤＢ３５に対応し、図１の受信手段２２、判定手段２３、および許可手段２４は、図２の認証局３４に対応する。

【００１５】

【発明の実施の形態】

以下、図面を参照しながら、本発明の実施の形態を詳細に説明する。

本実施形態の認証システムでは、独立した複数のネットワークサービスに対して、ユーザが１つのデジタル証明書を提示することで、それらのサービスの利用が許可される。このデジタル証明書は、所定の認証方法により認証されたユーザのみに対して発行され、そのユーザが複数のサービスを利用可能であることを表す。

【００１６】

デジタル証明書は、ＩＴＵ－Ｔ（International Telecommunication Union Telecommunication Standardization Sector）の仕様Ｘ．５０９に基づき、ユーザ名、証明書発行者名、シリアル番号、ユーザの公開鍵等の情報を統合したデータに、認証局（Certificate Authority ）のデジタル署名を施すことで生成される。この証明書は、中に収められている公開鍵がそこに記されたユーザのものであることを証明している。

【００１７】

図２は、このような認証システムにおけるデジタル証明書の発行と審査を示している。図２において、サービスＡ、Ｂは、ＩＤおよびパスワードを用いる会員制サービスに対応し、それぞれ、サーバ３２、３３からユーザ３１に対して提供される。認証局３４は、これらのサービスの事業体とは独立した証明書発行機関であり、ユーザ３１に対して、サービスＡ、Ｂに共通のデジタル証明書（共通証明書）を発行する。

【００１８】

共通証明書を用いた認証を可能にするためには、あらかじめ、認証局３４がユ

ーザ３１に対してその共通証明書を発行する必要がある。ここでは、認証局３４は、サービスＡを介して共通証明書を発行し、サービスＢに対する最初のアクセス時に、サーバ３３がその共通証明書を審査する。サーバ３２、３３は、それぞれ、ユーザ情報管理テーブル３６、３７を保持しており、これらのテーブルには、あらかじめ、ユーザ３１のＩＤ、パスワード等が登録されている。この場合、以下のシーケンスに従って処理が行われる。

【００１９】

Ｐ１：ユーザ３１は、サービスＡ用のＩＤおよびパスワードをサーバ３２に送る。サーバ３２は、ユーザ情報管理テーブル３６を参照してユーザ認証を行い、認証結果がＯＫであれば、認証局３４に共通証明書の発行を依頼する。

【００２０】

Ｐ２：サーバ３２は、認証局３４から共通証明書を受け取り、それをユーザ３１に対して発行する。この段階では、ユーザ３１が保持する共通証明書は、サービスＡを利用する資格のみを有し、認証局３４の証明書管理ＤＢ３５には、共通証明書の識別情報（例えば、シリアル番号）とともに、対応するユーザ名と、サービスＡが利用可能であることを示す情報が登録される。また、ユーザ情報管理テーブル３６には、ＩＤおよびパスワードとともに、その共通証明書のシリアル番号（Ｓｅｒ．Ｎｏ．）が登録される。

【００２１】

Ｐ３：ユーザ３１は、発行された共通証明書をサーバ３３に提示する。

Ｐ４：サーバ３３は、提示された共通証明書ではサービスＢが利用できないと判断し、ユーザ３１にサービスＢ用のＩＤおよびパスワードを要求する。

【００２２】

Ｐ５：ユーザ３１は、サービスＢ用のＩＤおよびパスワードをサーバ３３に送る。

Ｐ６：サーバ３３は、ユーザ情報管理テーブル３７を参照してユーザ認証を行い、認証結果がＯＫであれば、サービスＢをユーザ３１に提供する。これ以降、ユーザが保持する共通証明書でも、サービスＢの利用が可能となる。この段階では、ユーザが保持する共通証明書は、サービスＡとサービスＢを利用する資格を

有し、証明書管理ＤＢ３５には、サービスＡ、Ｂが利用可能であることを示す情報が登録される。また、ユーザ情報管理テーブル３７には、ＩＤおよびパスワードとともに、共通証明書のシリアル番号が登録される。

【００２３】

ここでは、Ｐ１およびＰ５の処理において、ＩＤおよびパスワードによるユーザ認証を行っているが、指紋情報、声紋情報、画像情報等による他の認証方法を用いてもよい。また、ユーザは、サービスの利用中止を希望する場合、共通証明書の失効またはサービスの利用禁止の手続きを行う。共通証明書の失効手続きを行う場合、図３に示すように、以下のシーケンスに従って処理が行われる。

【００２４】

Ｐ１１：ユーザ３１は、サービスＡ用のＩＤおよびパスワード、あるいは共通証明書を、サーバ３２に送る。

Ｐ１２：ＩＤおよびパスワードを受け取った場合、サーバ３２は、ユーザ情報管理テーブル３６を参照してユーザ認証を行い、認証結果がＯＫであれば、その旨をユーザ３１に通知する。また、共通証明書を受け取った場合、サーバ３２は、後述する認証方法でユーザ認証を行い、認証結果をユーザ３１に通知する。

【００２５】

Ｐ１３：ユーザ３１は、サーバ３２に対して、保持している共通証明書の失効依頼を行う。サーバ３２は、認証局３４に共通証明書のシリアル番号を通知し、失効処理を依頼する。認証局３４は、証明書管理ＤＢ３５からその共通証明書の情報を削除し、サーバ３２は、ユーザ情報管理テーブル３６からその共通証明書のシリアル番号を削除する。

【００２６】

Ｐ１４：その後、ユーザ３１は、保持している共通証明書を、認証情報としてサーバ３３に提示する。サーバ３３は、提示された共通証明書のシリアル番号を認証局３４に通知し、その共通証明書の正当性を問い合わせる。

【００２７】

Ｐ１５：認証局３４は、通知されたシリアル番号が証明書管理ＤＢ３５に登録されていないため、チェック結果がＮＧであることをサーバ３３に通知する。サ

ーバ３３は、ユーザ情報管理テーブル３７からその共通証明書のシリアル番号を削除し、サービスＢが利用不可であることをユーザ３１に通知する。

【００２８】

図４は、発行された共通証明書を用いたユーザ認証を示している。この場合、以下のシーケンスに従ってサービスが提供される。

Ｐ２１：ユーザ３１は、保持している共通証明書を、認証情報としてサーバ３２に提示する。サーバ３２は、提示された共通証明書のシリアル番号を認証局３４に通知し、その共通証明書のチェックを依頼する。認証局３４は、証明書管理ＤＢ３５を参照して、通知されたシリアル番号が登録されているか否かをチェックする。そして、そのシリアル番号が登録されており、かつ、サービスＡが利用可能であれば、チェック結果としてＯＫを返す。

【００２９】

Ｐ２２：サーバ３２は、認証局３４からＯＫが返されると、サービスＡをユーザ３１に提供する。

Ｐ２３：ユーザ３１は、保持している共通証明書を、認証情報としてサーバ３３に提示する。サーバ３３は、サーバ３２と同様にして、認証局３４からチェック結果を受け取る。

【００３０】

Ｐ２４：サーバ３３は、認証局３４からＯＫが返されると、サービスＢをユーザ３１に提供する。

ここでは、ユーザが２つのサービスを利用する場合について説明したが、３つ以上のサービスを利用する場合も同様である。また、サーバ３２、３３は、提示された共通証明書が失効しているか否かを確認するために、認証局３４に対して共通証明書のチェックを依頼しているが、このチェックを省略することも可能である。

【００３１】

この場合、失効処理において、認証局３４は、失効した共通証明書のシリアル番号を、関連するすべてのサービスのサーバに通知し、各サーバは、ユーザ情報管理テーブルからそのシリアル番号を削除する。そして、ユーザから共通証明書

が提示されたとき、そのシリアル番号が対応するユーザ情報管理テーブルに登録されていれば、認証結果をＯＫとし、それが登録されていなければ、認証結果をＮＧとする。

【００３２】

図２、３、および４に示した認証システムによれば、ユーザは、各サービス固有のＩＤおよびパスワードを使用することなく、単一の証明書を提示するだけで、複数のサービスを利用することができる。したがって、複数のＩＤおよびパスワードを暗記したり、サービス利用時に毎回ＩＤおよびパスワードを入力したりする必要がなくなり、ユーザの負担が大きく軽減される。

【００３３】

ところで、証明書管理ＤＢ３５には、例えば、図５のような証明書管理テーブルと、図６のような利用サービス管理テーブルが格納される。図５の証明書管理テーブルには、共通証明書のシリアル番号、ユーザの氏名、住所、およびｅメールアドレスが登録されており、図６の利用サービス管理テーブルには、共通証明書のシリアル番号および利用可能サービスＩＤが登録されている。証明書管理テーブルおよび利用サービス管理テーブルは、共通証明書毎に生成される。

【００３４】

また、図７は、ユーザ情報管理テーブル３６、３７の例を示している。図７のユーザ情報管理テーブルには、ユーザＩＤ、パスワード、ユーザの氏名、住所、および共通証明書のシリアル番号が登録されている。ユーザ情報管理テーブルは、ユーザ毎に生成される。

【００３５】

図８は、ユーザ３１がサービスＡのサーバ３２に対して、共通証明書の発行または失効を依頼する場合の処理のフローチャートである。まず、ユーザ３１は、サーバ３２にアクセスし（ステップＳ１）、サーバ３２は、ユーザ端末にログイン画面を表示する（ステップＳ２）。次に、ユーザ３１は、サービスＡ用のＩＤおよびパスワードを入力し（ステップＳ３）、サーバ３２は、ユーザ情報管理テーブル３６を参照して、入力されたＩＤおよびパスワードをチェックする（ステップＳ４）。

【００３６】

ＩＤおよびパスワードが正しくなければ、サーバ３２は、ステップＳ２以降の処理を繰り返す。ＩＤおよびパスワードが正しければ、次に、ユーザ情報管理テーブル３６を参照して、対応するユーザに対して共通証明書が発行されているか否かをチェックする（ステップＳ５）。

【００３７】

ユーザ情報管理テーブル３６に、そのユーザの共通証明書のシリアル番号が登録されていなければ、共通証明書が発行されていないと判断し、認証局３４に共通証明書の発行を依頼する（ステップＳ６）。

【００３８】

これを受けて、認証局３４は、共通証明書を発行する（ステップＳ７）。このとき、認証局３４は、共通証明書のシリアル番号とユーザ情報を記録した証明書管理テーブルを生成し、共通証明書のシリアル番号とサービスＡのＩＤを記録した利用サービス管理テーブルを生成する。そして、それらのテーブルを証明書管理ＤＢ３５に格納する。

【００３９】

次に、サーバ３２は、発行された共通証明書をユーザ３１に配布し、ユーザ情報管理テーブル３６に、共通証明書のシリアル番号を記録して（ステップＳ８）、処理を終了する。

【００４０】

ステップＳ５において、ユーザ情報管理テーブル３６に共通証明書のシリアル番号が登録されていれば、共通証明書が発行済みであることをユーザ３１に通知し、失効を希望するか否かを問い合わせる（ステップＳ９）。ユーザ３１が失効を希望しなければ、そのまま処理を終了する。

【００４１】

ユーザ３１が失効を希望すれば、登録されている共通証明書のシリアル番号を認証局３４に通知し、失効処理を依頼する（ステップＳ１０）。これを受けて、認証局３４は、通知されたシリアル番号に対応する証明書管理テーブルおよび利用サービス管理テーブルを削除し、処理結果をサーバ３２に通知する。そして、

サーバ３２は、ユーザ情報管理テーブル３６からその共通証明書のシリアル番号を削除し、共通証明書が失効したことをユーザ３１に通知して、処理を終了する。

【００４２】

次に、図９は、ユーザ３１がサービスＢのサーバ３３に対して、保持している共通証明書の審査を依頼する場合の処理のフローチャートである。まず、ユーザ３１は、サーバ３３にアクセスし（ステップＳ１１）、共通証明書を提示する（ステップＳ１２）。

【００４３】

次に、サーバ３３は、提示された共通証明書のシリアル番号がユーザ情報管理テーブル３７に登録されているか否かをチェックする（ステップＳ１３）。そして、そのシリアル番号が登録されていなければ、ステップＳ１４～Ｓ１６において、図８のステップＳ２～Ｓ４と同様の処理を行う。

【００４４】

ステップＳ１６において、ＩＤおよびパスワードが正しければ、次に、サーバ３３は、提示された共通証明書のシリアル番号を認証局３４に通知し、その共通証明書によるサービスＢの利用許可を要請する（ステップＳ１７）。

【００４５】

これを受けて、認証局３４は、通知されたシリアル番号に対応する利用サービス管理テーブルにサービスＢのＩＤを追加し、サービスＢが利用可能になったことをサーバ３３に通知する（ステップＳ１８）。そして、サーバ３３は、ユーザ情報管理テーブル3.7に、共通証明書のシリアル番号を記録して（ステップＳ１９）、処理を終了する。

【００４６】

ステップＳ１３において、共通証明書のシリアル番号がユーザ情報管理テーブル３７に登録されていれば、次に、サービスＢの利用を禁止するか否かをユーザ３１に問い合わせる（ステップＳ２０－１）。そして、ユーザ３１が利用禁止を希望しなければ、そのまま処理を終了する。

【００４７】

ユーザ３１が利用禁止を希望すれば、次に、提示された共通証明書のシリアル番号をユーザ情報管理テーブル３７から削除し（ステップＳ２０－２）、その共通証明書の利用可能サービスからサービスＢを抹消するように、認証局３４に依頼する（ステップＳ２０－３）。

【００４８】

これを受けて、認証局３４は、対応する利用サービス管理テーブルからサービスＢのサービスＩＤを削除し、サービスＢを抹消したことをサーバ３３に通知する（ステップＳ２０－４）。そして、サーバ３３は、サービスＢの利用が禁止されたことをユーザ３１に通知して、処理を終了する。

【００４９】

以上の説明では、証明書管理テーブルと利用サービス管理テーブルを別々に設けているが、これらのテーブルの情報を１つのテーブルにまとめて格納してもよい。

【００５０】

次に、図１０および図１１を参照しながら、インターネット上の会員制サービスであるｎｉｆｔｙにおいて、本発明の認証システムを適用した例を説明する。

現在、ｎｉｆｔｙと連動して各種分野のポータルサイト（portal site ）を構築し、多くの企業のサービスを提供する動きが見られる。ポータルサイトは、インターネットの入口となる巨大なＷｅｂサイトであり、様々なサービスサイトへのリンクを保持している。しかし、複数の独立したサービスをポータルサイトに集中させると、認証の煩雑さが大きな問題となる。これは、ｎｉｆｔｙに限らず、どのポータルサイトでも起こり得る問題である。このような場合に、上述した共通認証の仕組みを用いれば、複数のサービスによる認証が簡便化される。

【００５１】

図１０は、金融関連サービスを提供するポータルサイトＦｉｎａｎｃｅ＠ｎｉｆｔｙを含むサービスシステムの構成図である。図１０のサービスシステムは、インターネット４１、認証局のサーバ４２、＠ｎｉｆｔｙ会員サービスのサーバ４３、銀行のサーバ４４、クレジット会社のサーバ４５、保険会社のサーバ４６、インターネットショップのサーバ４７、電力会社のサーバ４８、ガス会社のサ

ーバ４９、およびユーザ端末５０を含む。

【００５２】

ここで、＠ｎｉｆｔｙ、銀行、クレジット会社、保険会社、インターネットショップ、電力会社、およびガス会社は、それぞれ、独立した会員制サービスを提供する事業体に相当する。

【００５３】

認証局のサーバ４２は、証明書管理ＤＢ３５、証明書管理部５１、およびサービス管理ＤＢ５２を備える。証明書管理ＤＢ３５は、各共通証明書の証明書管理テーブルおよび利用サービス管理テーブルを格納し、証明書管理部５１は、証明書管理ＤＢ３５を用いて、共通証明書の発行、チェック、失効等の処理を行う。また、サービス管理ＤＢ５２は、各サービスに関する情報を格納し、証明書管理部５１は、サービス管理ＤＢ５２を用いて、各サービスの入会審査に関する処理を行う。

【００５４】

また、＠ｎｉｆｔｙ会員サービスのサーバ４３は、会員画面制御部６１、請求管理部６２、ユーザ管理ＤＢ６３、画面レイアウトＤＢ６４、および請求情報ＤＢ６５を備える。ユーザ管理ＤＢ６３は、各ユーザのユーザ情報管理テーブルを格納し、画面レイアウトＤＢ６４は、会員サービス画面のデータを格納し、請求情報ＤＢ６５は、サーバ４７、４８、４９等から収集される請求金額のデータを格納する。

【００５５】

会員画面制御部６１は、ユーザ管理ＤＢ６３および画面レイアウトＤＢ６４を用いて、ユーザ端末５０上の画面表示を制御し、請求管理部６２は、請求情報ＤＢ６５を用いて、請求金額の表示を制御する。

【００５６】

例えば、ユーザ端末５０の画面に表示されたＦｉｎａｎｃｅ＠ｎｉｆｔｙのページ７１は、会員サービス８１および証明書８２の項目を含む。そして、ユーザがこれらの項目を指定すると、ユーザ端末５０が保持している共通証明書が自動的にサーバ４３に送られ、認証が行われて、会員メニューのページ７２が表示さ

れる。このページ７２には、公共料金決済サービス８３、明細表示サービス８４、転居手続きサービス８５、および会員設定８６の項目が含まれている。

【００５７】

このうち、ユーザが公共料金決済サービス８３を選択すると、共通証明書がサーバ４４に送られ、認証が行われて、公共料金決済のページ７３が表示される。このページ７３には、口座振替申込み８７、インターネット個別払い８８、および銀行決済申込み８９の項目が含まれている。

【００５８】

また、ユーザが明細表示サービス８４を選択すると、ユーザの金融情報の明細を示すページ７４が表示される。このとき、必要に応じて、共通証明書がサーバ４４、４５等にも送られ、認証が行われる。

【００５９】

このページ７４のレイアウトデータは、会員画面制御部６１から提供され、請求金額のデータは、請求管理部６２から提供される。さらに、銀行口座の残高データは、銀行のサーバ４４から提供され、クレジットカードの請求明細のデータは、クレジット会社のサーバ４５から提供される。

【００６０】

図１１は、図１０のサービスシステムにおいて、ユーザが明細表示サービス８４を利用する場合のシーケンスを示している。この処理においては、以下のシーケンスに従って、@ｎｉｆｔｙ、銀行、クレジット会社等の複数の事業体のサービスが複合的に提供される。

【００６１】

Ｐ３１：ユーザは、共通証明書を提示して、ユーザ端末５０からＦｉｎａｎｃｅ@ｎｉｆｔｙのサイトにアクセスする。

Ｐ３２：@ｎｉｆｔｙのサーバ４３は、提示された共通証明書のシリアル番号を、認証局のサーバ４２に通知する。

【００６２】

Ｐ３３：サーバ４２は、証明書管理ＤＢ３５の対応する利用サービス管理テーブルを参照し、その共通証明書で@ｎｉｆｔｙ会員サービスが利用可能であれば

、チェック結果としてＯＫを返す。

【００６３】

Ｐ３４：サーバ４３は、会員メニュー７２を表示する。

Ｐ３５：ユーザは、会員メニュー７２から明細表示サービスを選択する。

Ｐ３６：サーバ４３は、共通証明書のシリアル番号を認証局のサーバ４２に通知して、利用可能サービスを問い合わせる。

【００６４】

Ｐ３７：サーバ４２は、対応する利用サービス管理テーブルを参照して、通知されたシリアル番号に対応する利用可能サービスＩＤを取得し、それをサーバ４３に返す。

【００６５】

Ｐ３８：サーバ４３は、受け取った各サービスＩＤに対応する表示領域を含む、画面描画用のレイアウトデータをユーザ端末５０に送る。このレイアウトデータは、ＨＴＭＬ（hypertext markup language）、ＸＭＬ（extensible markup language）等で記述される。

【００６６】

Ｐ３９：ユーザ端末５０は、共通証明書を提示して、Ａ銀行のサーバに明細情報を問い合わせる。

Ｐ４０：Ａ銀行のサーバは、提示された共通証明書のシリアル番号を、認証局のサーバ４２に通知する。

【００６７】

Ｐ４１：サーバ４２は、証明書管理ＤＢ３５の対応する利用サービス管理テーブルを参照し、その共通証明書でＡ銀行のサービスが利用可能であれば、チェック結果としてＯＫを返す。

【００６８】

Ｐ４２：Ａ銀行のサーバは、ユーザ口座の残高データを、明細情報としてユーザ端末５０に送る。

Ｐ４３～Ｐ４６：Ｂ銀行のサーバも、Ａ銀行のサーバと同様にして、共通証明書による認証に基づいて、ユーザ口座の残高データをユーザ端末５０に送る。

【００６９】

こうして、ユーザ端末５０の画面に、明細ページ７４が表示される。クレジット会社のサーバ４５や保険会社のサーバ４６も、同様のシーケンスで、明細ページ７４に明細情報を提供することができる。

【００７０】

図１０のサービスシステムによれば、各サービスが別々に保持している口座残高や請求金額等の明細情報を、１つのレイアウト画面上に統合して表示することができ、複数のサービスの横断利用が可能になる。図１０においては、認証局の機能が各サービスから独立しているが、この機能を@ｎｉｆｔｙ会員サービスの中に取り込んでもよい。

【００７１】

図１０のサーバ４２～４９およびユーザ端末５０は、例えば、図１２に示すような情報処理装置（コンピュータ）を用いて構成することができる。図１２の情報処理装置は、ＣＰＵ（中央処理装置）９１、メモリ９２、入力装置９３、出力装置９４、外部記憶装置９５、媒体駆動装置９６、およびネットワーク接続装置９７を備え、それらはバス９８により互いに接続されている。

【００７２】

メモリ９２は、例えば、ＲＯＭ（read only memory）、ＲＡＭ（random access memory）等を含み、処理に用いられるプログラムとデータを格納する。ＣＰＵ９１は、メモリ９２を利用してプログラムを実行することにより、必要な処理を行う。

【００７３】

例えば、図１０の証明書管理部５１、会員画面制御部６１、および請求管理部６２は、プログラムにより記述されたソフトウェアコンポーネントとしてメモリ９２に格納される。

【００７４】

入力装置９３は、例えば、キーボード、ポインティングデバイス、タッチパネル等であり、オペレータ（サービス運用者またはユーザ）からの指示や情報の入力に用いられる。出力装置９４は、例えば、ディスプレイ、プリンタ、スピーカ

等であり、オペレータへの問い合わせや処理結果の出力に用いられる。

【００７５】

外部記憶装置９５は、例えば、磁気ディスク装置、光ディスク装置、光磁気ディスク（magneto-optical disk）装置、テープ装置等である。情報処理装置は、この外部記憶装置９５に、上述のプログラムとデータを保存しておき、必要に応じて、それらをメモリ９２にロードして使用する。また、外部記憶装置９５は、図１０の証明書管理ＤＢ３５、サービス管理ＤＢ５２、ユーザ管理ＤＢ６３、画面レイアウトＤＢ６４、および請求情報ＤＢ６５としても利用される。

【００７６】

媒体駆動装置９６は、可搬記録媒体９９を駆動し、その記録内容にアクセスする。可搬記録媒体９９としては、メモリカード、フロッピーディスク、ＣＤ－ＲＯＭ（compact disk read only memory）、光ディスク、光磁気ディスク等、任意のコンピュータ読み取り可能な記録媒体が用いられる。オペレータは、この可搬記録媒体９９に上述のプログラムとデータを格納しておき、必要に応じて、それらをメモリ９２にロードして使用する。

【００７７】

ネットワーク接続装置９７は、インターネット４１等の任意の通信ネットワークに接続され、通信に伴うデータ変換を行う。また、情報処理装置は、上述のプログラムとデータをネットワーク接続装置９７を介して他の装置から受け取り、必要に応じて、それらをメモリ９２にロードして使用する。

【００７８】

図１３は、図１２の情報処理装置にプログラムとデータを供給することのできるコンピュータ読み取り可能な記録媒体を示している。可搬記録媒体９９や外部のデータベース１００に保存されたプログラムとデータは、メモリ９２にロードされる。そして、ＣＰＵ９１は、そのデータを用いてそのプログラムを実行し、必要な処理を行う。

【００７９】

以上説明した実施形態においては、ＩＴＵ－Ｔの仕様Ｘ．５０９に基づくデジタル証明書を認証情報として用いているが、必要に応じて、他の仕様の証明書情

報を用いてもよい。

【００８０】

【発明の効果】

本発明によれば、複数のサービスに共通の１つの認証情報により、各サービスによる認証が可能になる。このため、ユーザは、各サービスが発行するＩＤおよびパスワードを使い分ける必要がなくなり、ユーザの負担が軽減される。また、異なるサービス間でパスワード等を互いに知らせる必要がなく、セキュリティが保持される。

【図面の簡単な説明】

【図１】

本発明の認証システムの原理図である。

【図２】

証明書の発行と審査を示す図である。

【図３】

証明書の失効を示す図である。

【図４】

証明書による認証を示す図である。

【図５】

証明書管理テーブルを示す図である。

【図６】

利用サービス管理テーブルを示す図である。

【図７】

ユーザ情報管理テーブルを示す図である。

【図８】

証明書の発行／失効処理のフローチャートである。

【図９】

証明書の審査処理のフローチャートである。

【図１０】

サービスシステムの構成図である。

【図１１】

複数サービスの利用例を示す図である。

【図１２】

情報処理装置の構成図である。

【図１３】

記録媒体を示す図である。

【図１４】

従来のサービスシステムを示す図である。

【符号の説明】

１１、３１　ユーザ

１２、３２　サービスＡのサーバ

１３、１５　ユーザ管理ＤＢ

１４、３３　サービスＢのサーバ

２１　登録手段

２２　受信手段

２３　判定手段

２４　許可手段

３４　認証局

３５　証明書管理ＤＢ

３６、３７　ユーザ情報管理テーブル

４１　インターネット

４２　認証局のサーバ

４３　＠ｎｉｆｔｙ会員サービスのサーバ

４４　銀行のサーバ

４５　クレジット会社のサーバ

４６　保険会社のサーバ

４７　インターネットショップのサーバ

４８　電力会社のサーバ

４９　ガス会社のサーバ

５０　ユーザ端末

５１　証明書管理部

５２　サービス管理ＤＢ

６１　会員画面制御部

６２　請求管理部

６３　ユーザ管理ＤＢ

６４　画面レイアウトＤＢ

６５　請求情報ＤＢ

７１　ｆｉｎａｎｃｅ＠ｎｉｆｔｙのページ

７２　会員メニューのページ

７３　公共料金決済のページ

７４　明細ページ

８３　公共料金決済サービス

８４　明細表示サービス

８５　転居手続きサービス

８６　会員設定

８７　口座振替申込み

８８　インターネット個別払い

８９　銀行決済申込み

９１　ＣＰＵ

９２　メモリ

９３　入力装置

９４　出力装置

９５　外部記憶装置

９６　媒体駆動装置

９７　ネットワーク接続装置

９８　バス

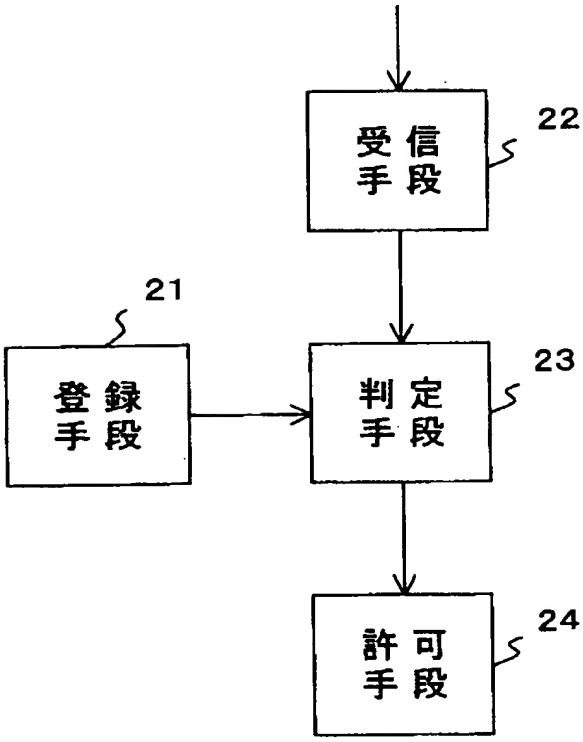
９９　可搬記録媒体

１００　データベース

【書類名】　　図面

【図１】

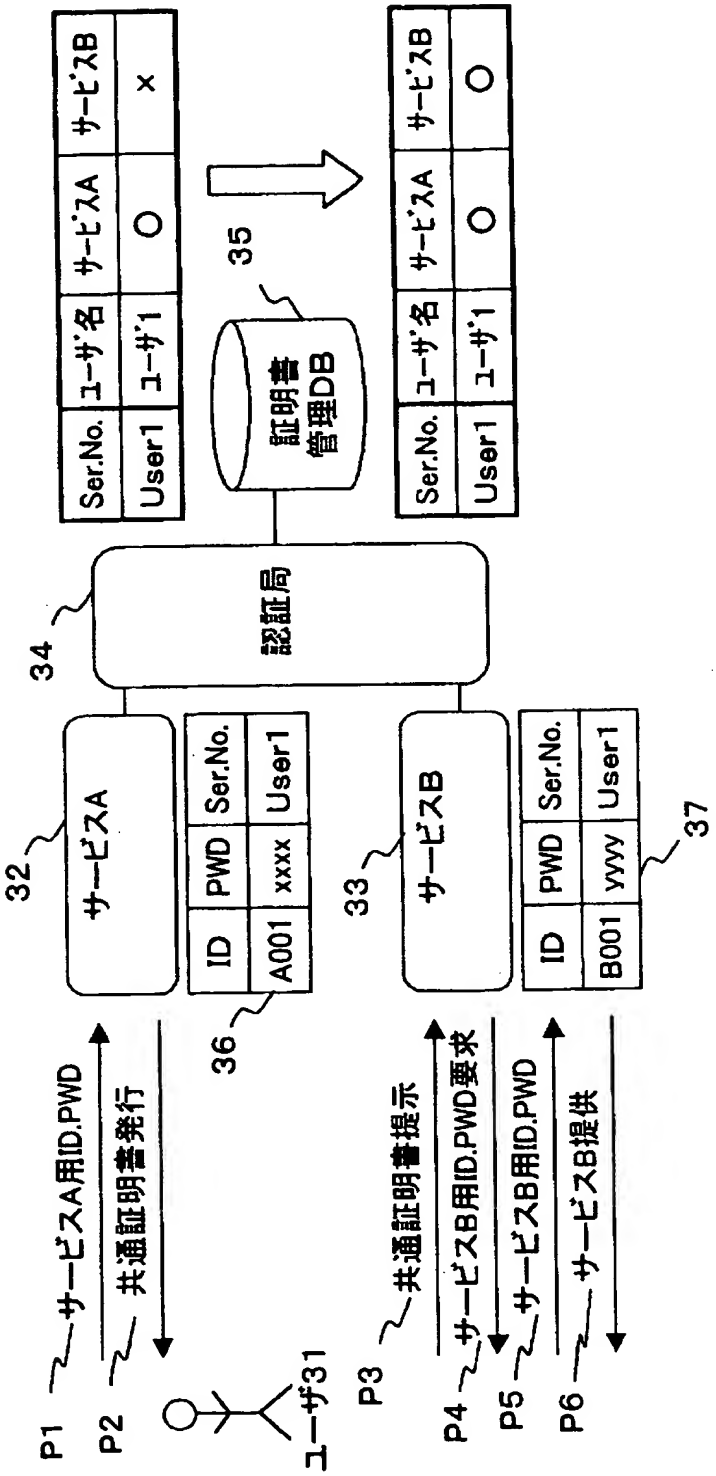
本　発　明　の　原　理　図



【図２】

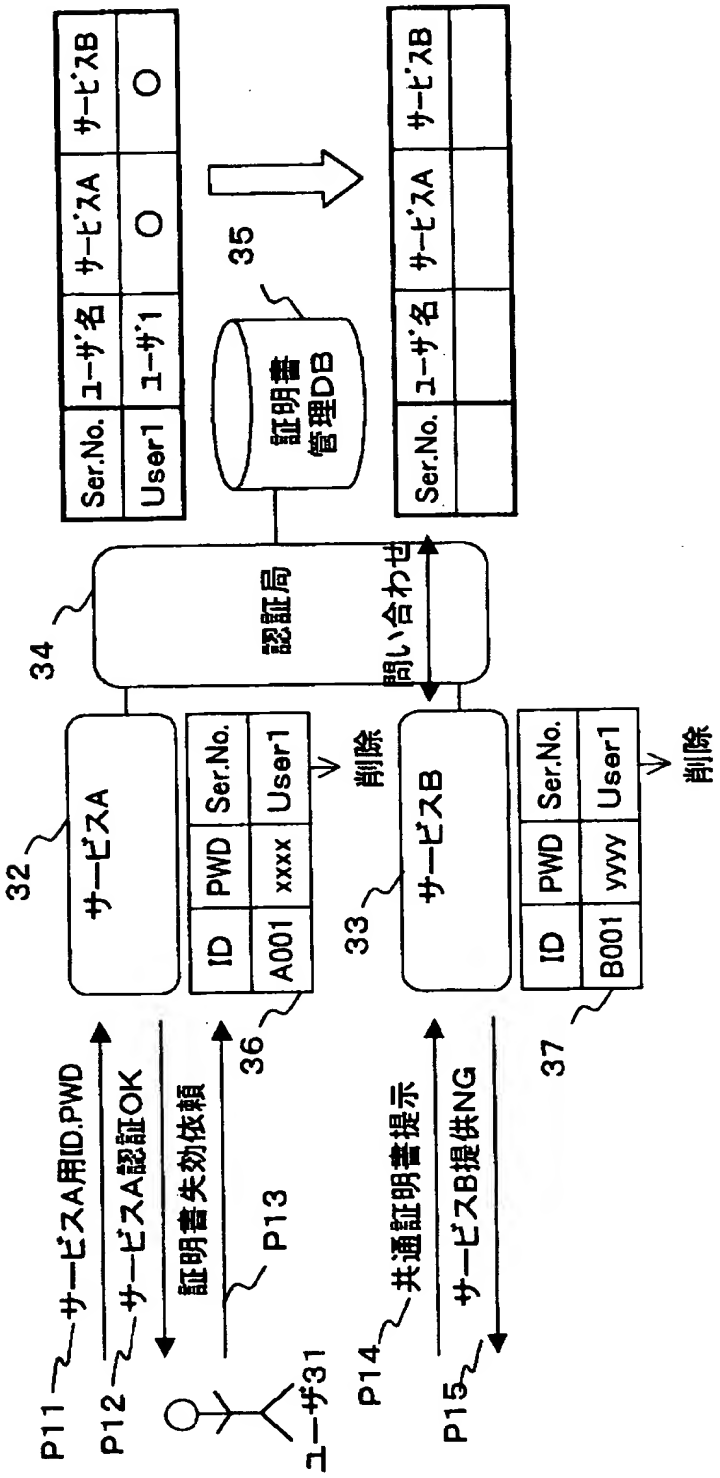
出証特２０００－３０７９６８２

証明書の発行と審査を示す図



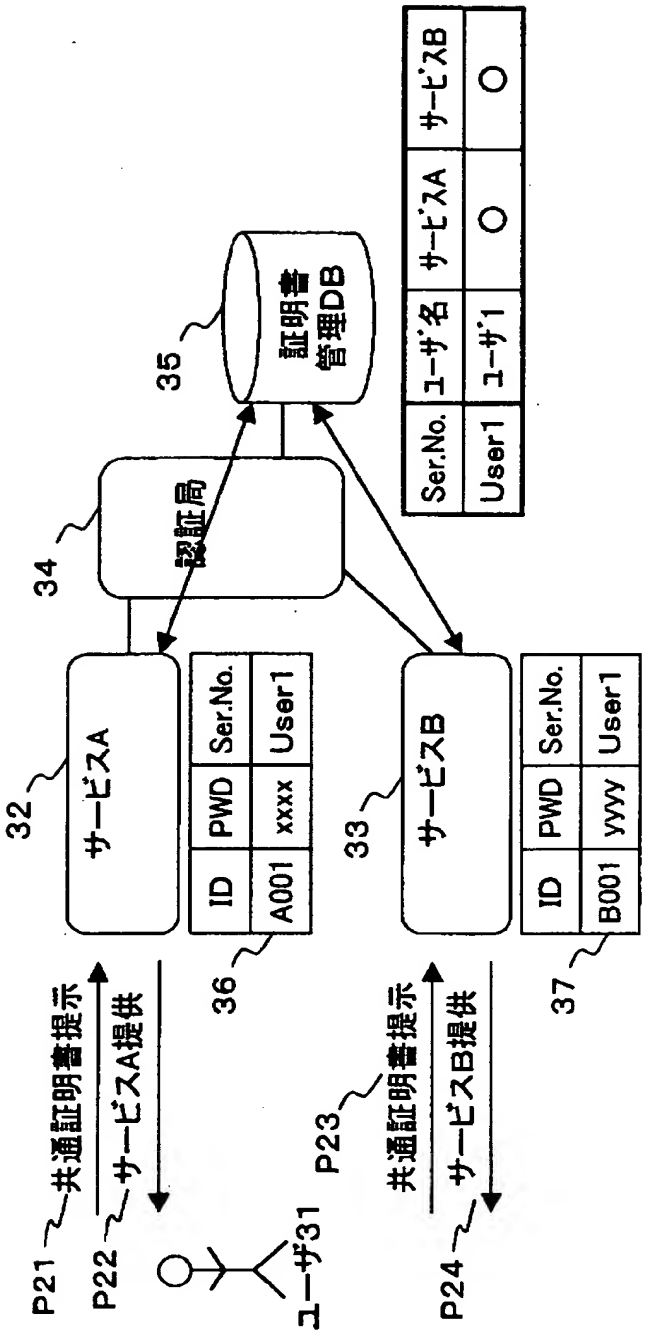
【図３】

証明書の失効を示す図



【図４】

証明書による認証を示す図



【図５】

証明書管理テーブルを示す図

証明書Ser. No.	User0001
氏名	富士通太郎
住所	東京都大田区
eメールアドレス	xxx@xxx. jp

【図６】

利用サービス管理テーブルを示す図

証明書Ser. No.	User0001
利用可能サービスID	Service A Service B

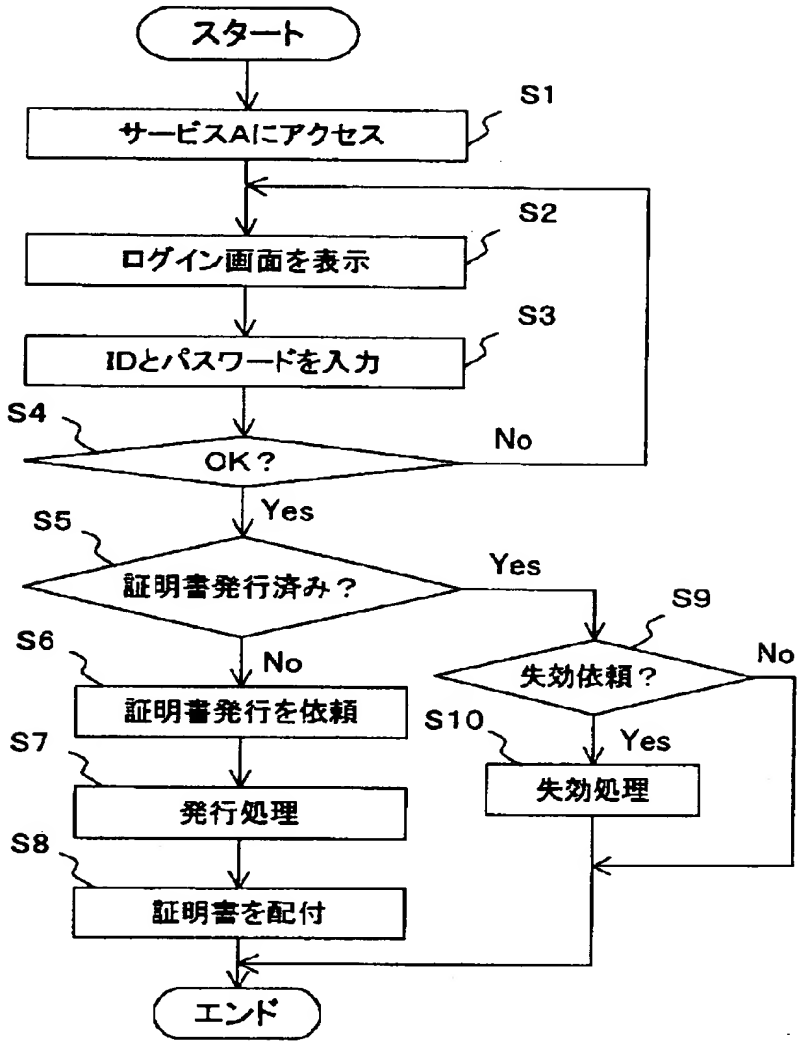
【図７】

ユーザ情報管理テーブルを示す図

ユーザID	AAA00000
パスワード	XXXXXXXX
氏名	富士通太郎
住所	東京都大田区
証明書Ser. No.	User0001

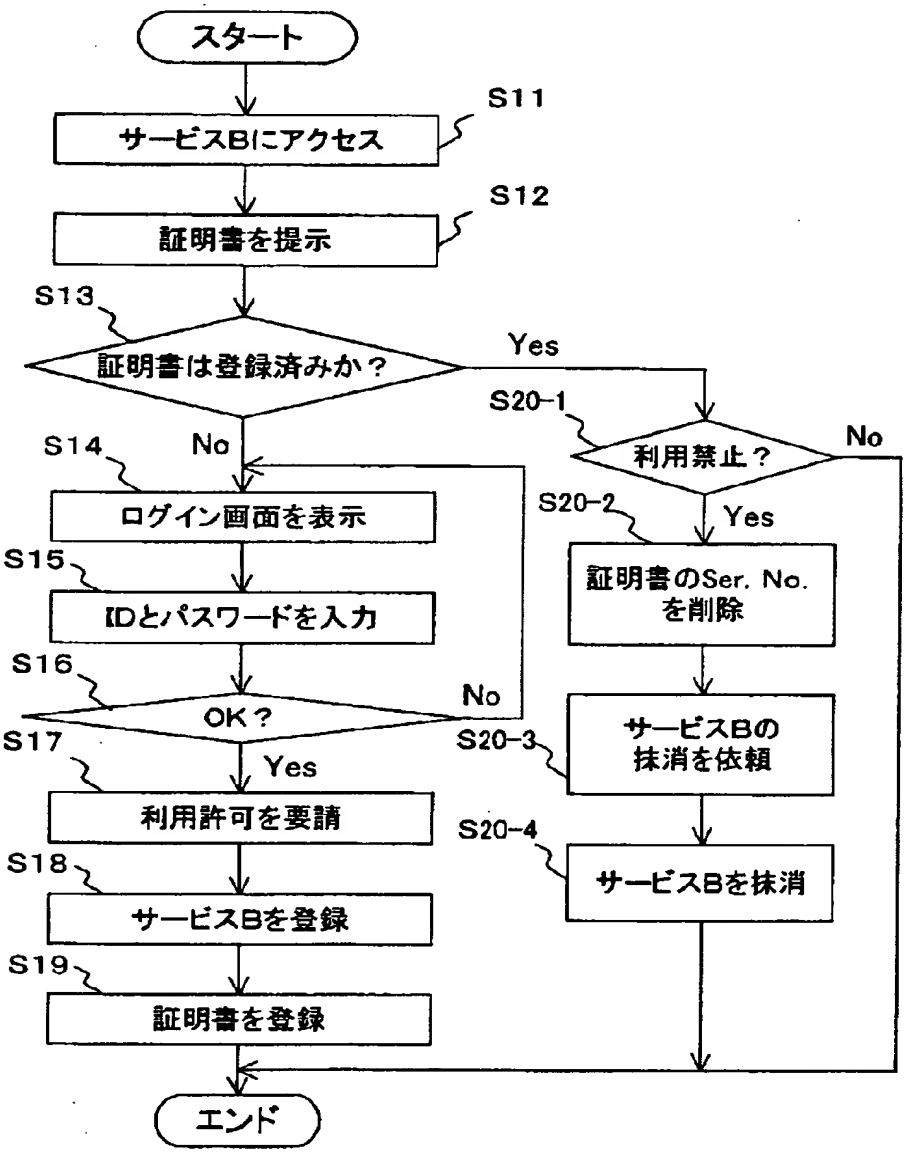
【図８】

証明書の発行／失効処理のフローチャート



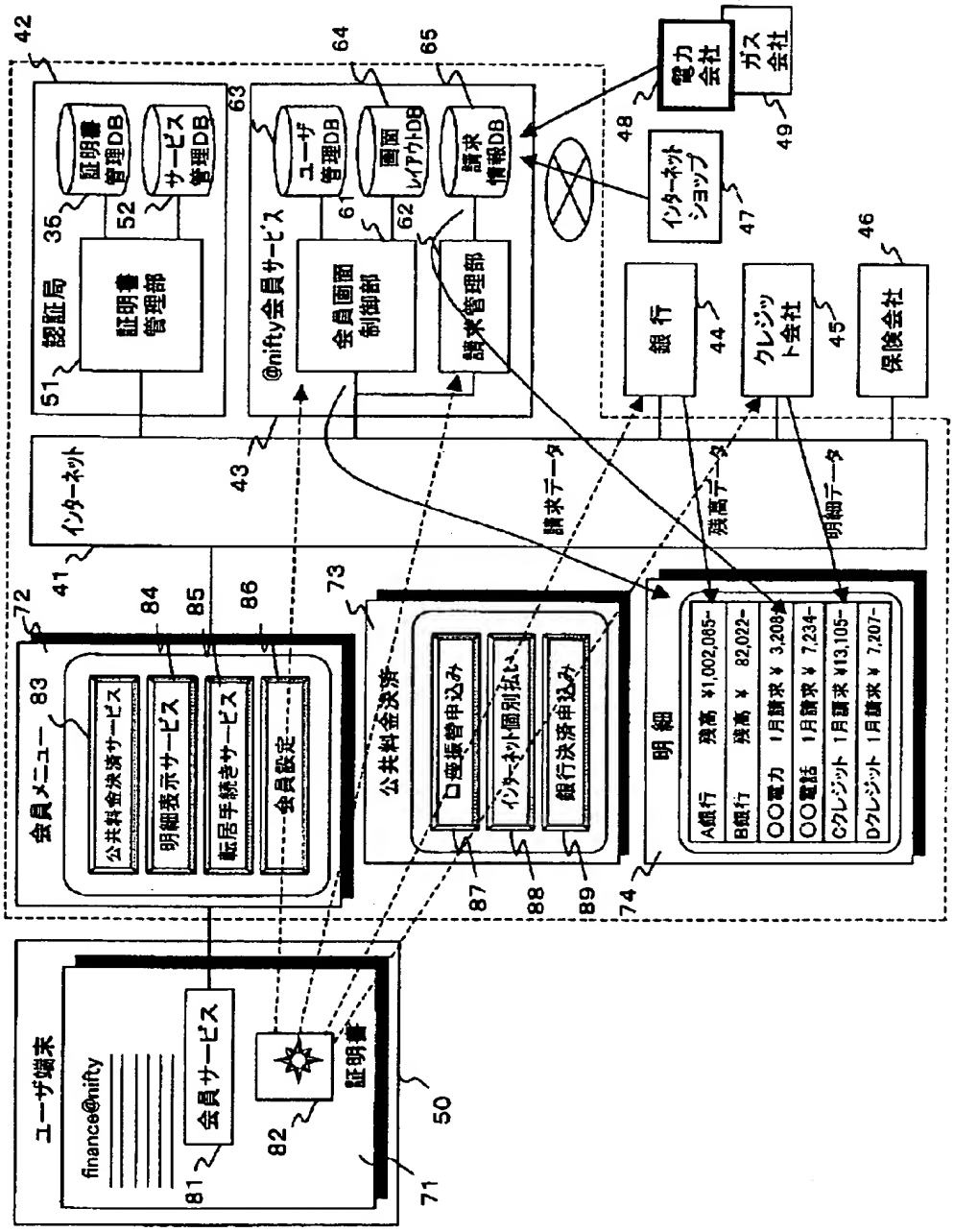
【図９】

証明書の審査処理のフローチャート



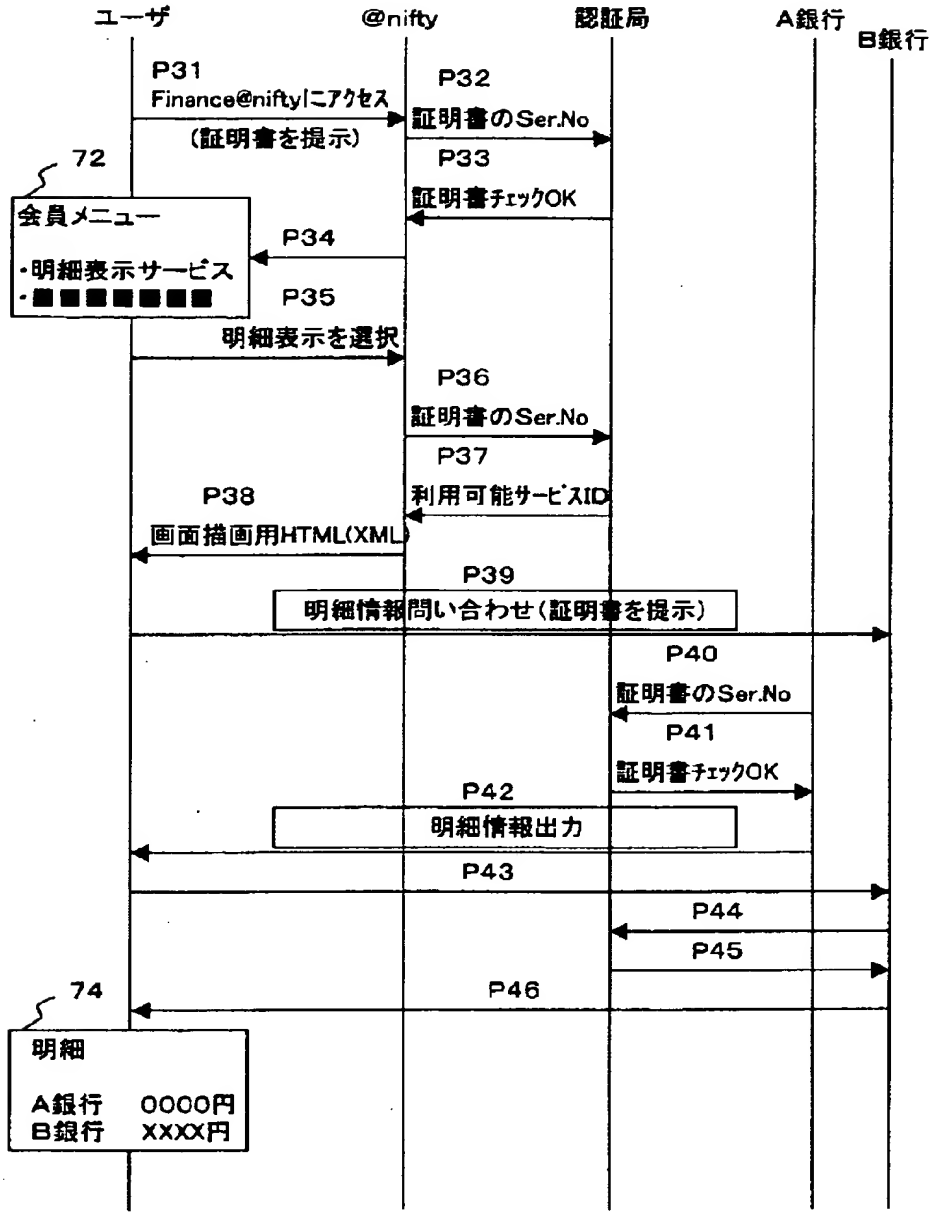
【図１０】

サービスシステムの構成図



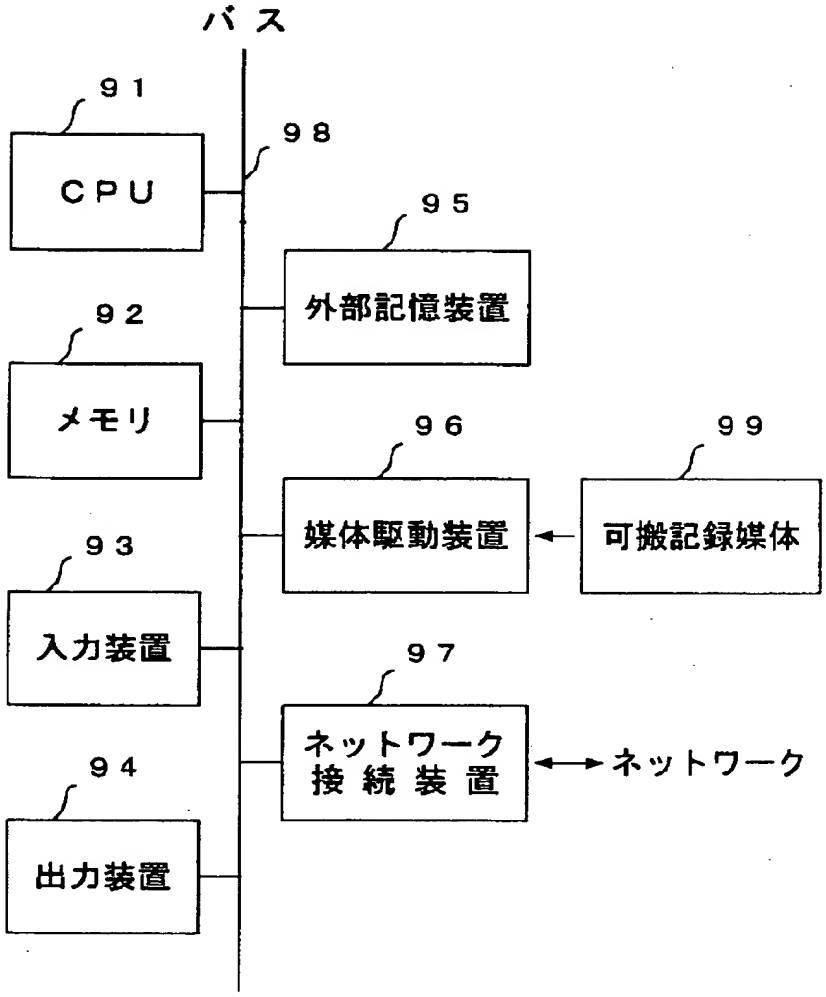
【図１１】

複数サービスの利用例を示す図



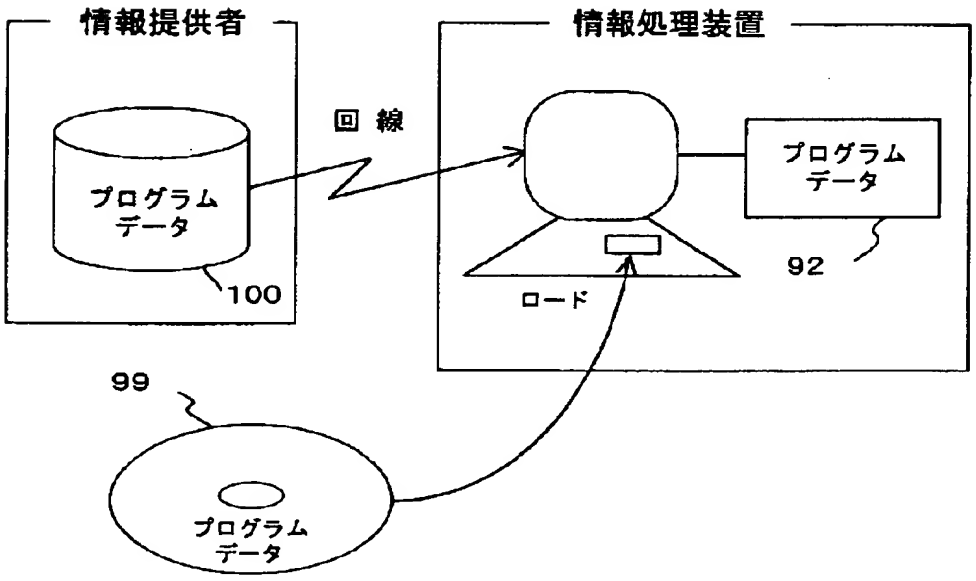
【図１２】

情　報　処　理　装　置　の　構　成　図



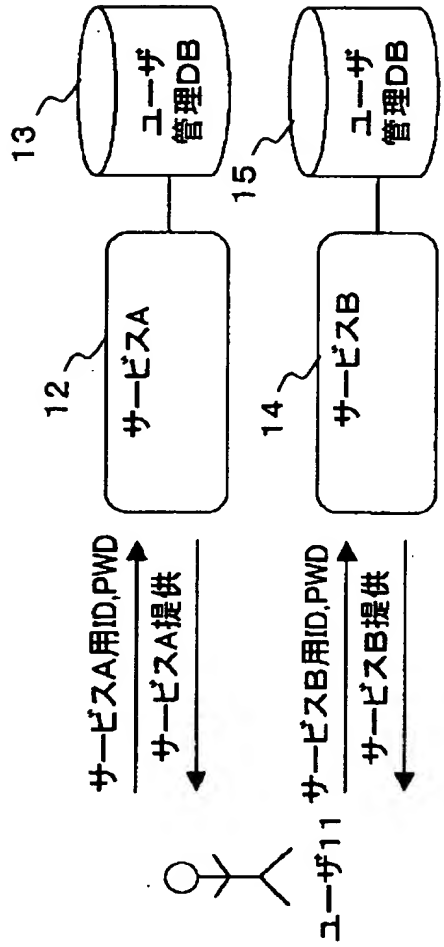
【図１３】

記　録　媒　体　を　示　す　図



【図１４】

従来のサービスシステムを示す図



【書類名】　　要約書

【要約】

【課題】　ネットワーク上の複数のサービスのための認証処理において、ユーザの負担を軽減することが課題である。

【解決手段】　ユーザ３１は、共通証明書をサービスＡのサーバ３２に提示し（Ｐ２１）、サーバ３２は、提示された共通証明書のシリアル番号を認証局３４に通知する。認証局３４は、証明書管理ＤＢ３５を参照して、通知されたシリアル番号が登録されており、かつ、サービスＡが利用可能であれば、ＯＫを返す。これを受けて、サーバ３２は、サービスＡをユーザ３１に提供する（Ｐ２２）。同様にして、ユーザ３１が共通証明書をサービスＢのサーバ３３に提示すると（Ｐ２３）、サーバ３３は、サービスＢをユーザ３１に提供する（Ｐ２４）。

【選択図】　　図４

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
　［変更理由］　住所変更
　　住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
　　氏　名　　富士通株式会社